



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Amo

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/875,261	06/05/2001	Todd F. Mozer	016757-000800US	4605

7590

09/13/2004

Chad Walsh, Esq.
Fountainhead Law Group
6172 Bollinger Road, #174
San Jose, CA 95129

EXAMINER

LERNER, MARTIN

ART UNIT PAPER NUMBER

2654

DATE MAILED: 09/13/2004

7

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/875,261

Applicant(s)

MOZER, TODD F.

Examiner

Martin Lerner

Art Unit

2654

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 to 43 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1 to 43 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 June 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

Drawings

1. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings are informal. The drawings are informal because they contain hand numbering of elements and steps, and because they are stated to be informal in the Application Data Sheet. Applicant is advised to employ the services of a competent patent draftsman outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Specification

2. The disclosure is objected to because of the following informalities:

On page 18, line 7, "1002" should be —1003—. See Figure 10.

Appropriate correction is required.

Claim Objections

3. Claims 31 to 43 are objected to because of the following informalities:

Independent claim 31, line 10, "biometric being" should be —biometric data being—. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1 to 4, 6, 9 to 14, 16 to 19, 22 to 24, 31, 35, 36, 40, 41, and 43 are rejected under 35 U.S.C. 102(e) as being anticipated by *Weideman*.

Regarding independent claim 1, *Weideman* discloses a speech recognition and verification system having a client unit and server unit, comprising:

“a client system receiving first biometric data and having a first level security authorization procedure” – transformed speech data (“first biometric data”) may be initially recognized (“a first level security authorization procedure”) to confirm that the identifier can be correctly identified by the speech recognizer prior to transmission of the data from client unit 10 to server unit 12 (column 3, lines 51 to 59: Figure 2a: Step 31); Figure 2a illustrates a method wherein recognition of the identifier is confirmed before transmission to the local server (column 3, lines 20 to 23: Figures 1 and 2a);

“a server system receiving second biometric data and having a second level security authorization procedure” – the encrypted data (“second biometric data”) is then transferred to the server unit 12 wherein the speech recognition and verification engines

Art Unit: 2654

22 are used to recognize the transmitted information and verify the user (“a second level security authorization procedure”) transmitting the information has authority to request a transaction using the spoken identifier (column 3, line 66 to column 4, line 4: Figures 2a and 2b: Step 38);

“wherein the first level security authorization procedure and the second level security authorization procedure comprise distinct biometric algorithms” – client unit 10 performs a speech feature application 20 to transform the speech data representing the phrase from the microphone 18 into speech feature data, and uses a speech recognition algorithm to determine whether the data is properly recognized, and then may prompt the user to reenter the phrase or identifier (column 3, lines 35 to 59: Figure 2a); server unit 12 recognizes the transmitted information with speech recognition and verification engines 22 to verify the user (column 3, line 66 to column 4, line 4: Figures 2a and 2b); implicitly, an algorithm performing speech feature extraction and speech recognition at a client is distinct from an algorithm performing speech recognition and verification at the server.

Regarding independent claim 9, *Weideman* discloses a method for performing speech recognition and verification on a system having a client unit and server unit, comprising:

“receiving a first level security authorization signal on the server system from a client system” – transformed speech data may be initially recognized to confirm that the identifier can be correctly identified by the speech recognizer prior to transmission of the

Art Unit: 2654

data from client unit 10 to server unit 12 (column 3, lines 51 to 59: Figure 2a: Step 31); Figure 2a illustrates a method wherein recognition of the identifier is confirmed before transmission to the local server (column 3, lines 20 to 23: Figures 1 and 2a); transmission of a confirmed recognition identifier is “a first level security authorization signal” sent by client unit 10 and received by server unit 12;

“receiving biometric data on the server system from the client system” – the encrypted data (“biometric data”) is then transferred from client unit 10 to the server unit 12 (column 3, line 66 to column 4, line 4: Figures 2a and 2b: Step 38);

executing a second level security authorization, the second level security authorization including analyzing the biometric data using a first biometric algorithm on the server system” – the speech recognition and verification engines 22 (“a first biometric algorithm”) are used to recognize (“analyzing the biometric data”) the transmitted information (“the biometric data”) and verify the user (“the second level security authorization”) transmitting the information has authority to request a transaction using the spoken identifier (column 3, line 66 to column 4, line 4: Figures 2a and 2b: Step 38);

“generating a second level security authorization signal on the server system when the first biometric algorithm indicates that the biometric data corresponds to one of a plurality of users authorized to access the server system” – if the transmitted information and the identity of the user are verified, the transaction is confirmed (column 4, lines 29 to 31: Figures 2a and 2b: Step 42).

Art Unit: 2654

Regarding independent claim 31, *Weideman* discloses a method for performing speech recognition and verification on a system having a client unit and server unit, comprising:

“receiving biometric data in the client system” – speech feature application 20 in client unit 10 receives a spoken key phrase or identifier (“biometric data”) (column 3, lines 35 to 39; Figures 1 and 2a: Steps 24 to 28);

“analyzing a first portion of the biometric data using a first biometric algorithm on the client system” – the speech feature application 20 (“a first biometric algorithm”) transforms the speech data (“analyzing a first portion of the biometric data”) representing the phrase from the microphone 18 into speech feature data used for recognition and verification (column 3, lines 39 to 50; Figures 1 and 2a: Step 30)

“generating a first level security authorization signal on the client system when the first biometric algorithm indicates that the first portion of the biometric data corresponds to an authorized user” – transformed speech data may be initially recognized to confirm that the identifier can be correctly identified by the speech recognizer prior to transmission of the data from client unit 10 to server unit 12 (column 3, lines 51 to 59; Figure 2a: Step 31); Figure 2a illustrates a method wherein recognition of the identifier is confirmed before transmission to the local server (column 3, lines 20 to 23; Figures 1 and 2a); transmission of a confirmed recognition identifier is “generating a first level security authorization signal” sent by client unit 10 and received by server unit 12;

“transmitting the first level security authorization signal and second portion of the biometric data to a server system, the second portion of biometric being analyzed by a second biometric algorithm on the server” – transmission of a confirmed recognition identifier from client 10 to server 12 is “generating a first level security authorization signal”; a determination is made whether or not the spoken identifier has been correctly recognized by the recognition algorithm at server 12; this may be done by asking the user to repeat the spoken identifier (“second portion of the biometric data”) (column 4, lines 5 to 14: Figures 2a and 2b: Step 39); verification routine 66b includes a TEST output for initiating prompting wherein additional follow-up questions (“second portion of the biometric data”) are asked to verify the user’s identity (“analyzed by a second biometric algorithm”) (column 6, lines 1 to 8: Figure 3);

“accessing resources on the server system through the client system when the second biometric algorithm provides a second level security authorization” – the speech recognition and verification engines 22 (“the second biometric algorithm”) are used to recognize the transmitted information and verify the user (“a second level security authorization”) transmitting the information has authority to request a transaction using the spoken identifier (column 3, line 66 to column 4, line 4: Figures 2a and 2b: Step 38); if the transmitted information and the identity of the user are verified, the transaction is confirmed (“authorizing resources”) (column 4, lines 29 to 31: Figures 2a and 2b: Step 42).

Art Unit: 2654

Regarding claims 2 to 4, and 41, *Weideman* discloses all biometric data is speech data or a speech utterance, and can be a password (column 3, lines 35 to 39).

Regarding claims 6 and 40, *Weideman* discloses speech recognition and verification engines 22 ("the second level of security authorization") at server 12 verify the user ("user identification") (column 3, line 66 to column 4, line 4: Figures 2a and 3).

Regarding claims 10 and 11, *Weideman* discloses transformed speech data may be initially recognized to confirm that the identifier can be correctly identified by the speech recognizer prior to transmission of the data from client unit 10 to server unit 12 (column 3, lines 51 to 59: Figure 2a: Step 31); transmission of a confirmed recognition identifier is "the first level security authorization signal" sent by client unit 10 and recognized by client unit with a recognition algorithm ("a second recognition algorithm on the client"); if the data is not properly recognized ("user has not been authorized") at the client, the user is prompted to reenter the phrase or identifier (column 3, lines 58 to 59: Figure 2a: Step 28); the absence of confirmed recognition is "the first level security authorization signal indicates that a user has not been authorized".

Regarding claim 12, *Weideman* discloses a determination is made whether or not the spoken identifier has been correctly recognized by the recognition algorithm at server 12; this may be done by asking the user to repeat the spoken identifier ("re-executing the second level security authorization") (column 4, lines 5 to 14: Figures 2a and 2b: Step 39).

Regarding claim 13, *Weideman* discloses transformed speech data may be initially recognized to confirm that the identifier can be correctly identified by the speech

Art Unit: 2654

recognizer prior to transmission of the data from client unit 10 to server unit 12 (column 3, lines 51 to 59: Figure 2a: Step 31); transmission of a confirmed recognition identifier is "control information" sent by client unit 10 and received by server unit 12.

Regarding claims 14, 16, and 17, *Weideman* discloses a decision routine 66a evaluates a measure of word similarity ("verification confidence value") for each of the digits (column 5, lines 31 to 52: Figure 3); verifier routine 66b generates one of three different outputs: ACCEPT, REJECT and TEST ("verification confidence value") (column 6, lines 1 to 7: Figure 3); the TEST output initiates the prompting step wherein additional follow-up questions are asked to verify the user's identity ("prompting the user for additional biometric information").

Regarding claims 18, 19, 35, and 36, *Weideman* discloses an objective of limiting access to a payment gateway for credit card authorization (column 6, lines 17 to 51: Figures 4a and 4b).

Regarding claims 22 and 23, *Weideman* discloses authorizing access to a payment gateway and merchant server (column 6, lines 17 to 51: Figures 4a and 4b); implicitly, there are a plurality of merchants and merchant servers providing remote resources.

Regarding claim 24, *Weideman* discloses verifier routine 66b generates one of three different outputs: ACCEPT, REJECT and TEST ("verification confidence value"); the TEST output initiates the prompting step wherein additional follow-up questions are asked to verify the user's identity (column 6, lines 1 to 7: Figure 3); prompting with follow-up questions is "an identification script".

Art Unit: 2654

Regarding claim 43, *Weideman* discloses the user may enter their credit card number via a magnetic card reader terminal (column 6, lines 45 to 51); a credit card is a "smart card".

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 7, 8, 15, 32 to 34, 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Weideman* in view of *Su et al.*

Concerning claims 7 and 8, *Weideman* does not expressly disclose security authorizations with a neural network and Hidden Markov Models. However, it is well known that speech recognition and verification algorithms utilize neural networks and Hidden Markov Models as alternative ways of performing speech recognition and verification. Specifically, *Su et al.* teaches creating speaker models by neural networks and Hidden Markov Models. (Column 6, Lines 1 to 10) It would have been obvious to one having ordinary skill in the art to utilize neural networks and Hidden Markov Models as taught by *Su et al.* in the speech recognition and verification system of *Weideman* because it is well known that these are the main algorithms for performing recognition and verification.

Art Unit: 2654

Concerning claims 32 and 38, *Weideman* discloses client unit 10 performs speech recognition but not speaker verification, and server unit 12 generates confidence values but not client unit 10. However, it is well known to distribute processing functions between a client and server in a speech recognition system, and *Weideman* suggests performing some speech processing and identifier confirmation at the client. It would have been obvious to one having ordinary skill in the art to generate confidence values and perform speaker recognition in the client of *Weideman* because it is well known to distribute functions between the client and server in speech recognition systems.

Concerning claims 15 and 33, *Weideman* does not disclose modifying an acceptance threshold. However, *Su et al.* teaches a security application, where a user can select a desired level of security and threshold levels are adjusted to accommodate the particular level of security desired. (Column 8, Line 59 to Column 9, Line 7: Figure 4) *Su et al.* states an advantage is maintaining a high level of security that alleviates the problem of requiring the user to memorize passwords. (Column 1, Lines 29 to 47) It would have been obvious to one having ordinary skill in the art to modify a threshold level in a speaker verification system as suggested by *Su et al.* in the speech recognition and verification system of *Weideman* for the purpose of alleviating the problem of requiring the user to memorize passwords.

Concerning claim 34, *Weideman* discloses an evaluation of word similarity by decision routine 66a, and outputting ACCEPT, REJECT and TEST by verifier routine 66b, as "confidence values" defining "ranges" (column 6, lines 1 to 7: Figure 3).

Concerning claim 39, *Weideman* discloses biometric data is a password (column 3, lines 35 to 39).

8. Claims 20, 21, and 37 rejected under 35 U.S.C. 103(a) as being unpatentable over *Weideman* in view of *Gifford*.

Weideman discloses authorizing access to a payment gateway and merchant server (column 6, lines 17 to 51: Figures 4a and 4b), but does not specifically provide authorization criteria of spending amount limitations or allowable network connection time. However, *Gifford* teaches an open network payment system, where authentication is provided for spending limits for any duration of time so as to limit fraud risk. (Column 8, Line 65 to Column 9, Line 18) Implicitly, limiting a spending amount for any duration of time involves limiting network connection time when a purchase involves computer network time. It would have been obvious to one having ordinary skill in the art to provide for spending limits and limiting allowable network connection time as suggested by *Gifford* in the speech recognition and verification system of *Weideman* for the purpose of limiting fraud risk.

9. Claims 25 to 27 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Weideman* in view of *Kanevsky et al.*

Concerning claims 25 to 27, *Weideman* does not expressly disclose storing biometric data on a server, wherein the biometric data is a finger print or voice print. Implicitly, however, a speaker verification system requires pre-stored data to compare

Art Unit: 2654

with a user's speech for verification, and the pre-stored data is commonly called a voice print. However, *Kanevsky et al.* teaches a method of providing secure access control, where the input device can be a fingerprint reader (column 3, lines 57 to 58; column 4, lines 17 to 18), and training to interpret the voice of the user is typically accomplished by storing the user's data for subsequent interpretation (column 4, line 65 to column 5, line 16). *Kanevsky et al.* states an advantage of improved security in controlling access to a service or facility with a relatively small database. (Column 1, Lines 59 to 65) It would have been obvious to one having ordinary skill in the art to provide for pre-stored data on a server as a typical way to recognize voice prints and finger prints as taught by *Kanevsky et al.* in the speech recognition and verification system of *Weideman* for the purpose of improving security in a controlled access facility with a relatively small database.

Concerning claim 42, *Kanevsky et al.* suggests verifying access to a video provider (column 1, lines 14 to 23), and a wireless link (column 3, lines 59 to 65) providing portability, equivalent to a "portable media player".

10. Claims 28 to 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Weideman* in view of *Su et al.* as applied to claim 9 above, and further in view of *Maurer et al.*

Su et al. suggests background noise conditions affect speaker verification (column 6, lines 60 to 67), changing recognition algorithms by varying the script (column 8, lines 27 to 58), and changing recognition parameters by adjusting the threshold

Art Unit: 2654

(column 8, line 59 to column 9, line 7). However, *Su et al.* omits changing recognition algorithms and recognition parameters based upon line quality measures. *Maurer et al.* teaches evaluating the quality of a transmission channel using voice recognition for the purpose of providing a powerful and effective tool for testing applications. (Column 2, Lines 28 to 54) It would have been obvious to one having ordinary skill in the art to evaluate line quality as suggested by *Maurer et al.* to change recognition algorithms and recognition parameters as taught by *Su et al.* for the purpose of providing a tool for testing and improving a speaker verification system due to changing background noise conditions.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure.

Chadha, Talmor et al., and Moser et al. disclose related art.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Martin Lerner whose telephone number is (703) 308-9064. The examiner can normally be reached on 8:30 AM to 6:00 PM Monday to Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Richemond Dorvil can be reached on (703) 305-9645. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2654

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ML
9/7/04


Martin Lerner
Examiner
Group Art Unit 2654